Alexander Wiegman

Remote, USA (and sometimes Japan) | hello@madicetea.me | (209)-353-5377 | https://github.com/madicetea

Summary

Alex is an experienced analyst with a passion for computing systems, architectures, networks, and their security. He currently is pursuing a challenge to discover and apply concepts of compliance, security controls, and systems architecture to become an overall better security engineering professional in the solutions / security architecture fields.

Work Experience

GRC Analyst **Kong Inc. (San Francisco, USA)** **08/2021 – (current)**

The most popular open-source API gateway solutions for microservices, self-hosted or in cloud. | *https://konghq.com*

- Automate, test, and train compliance questionnaires & documentation using industry workflow software and procedures.
- Contribute to compliance & business efforts from research on recent industry regulations, governmental policies, and laws.
- Evaluate between and implement competing choices for technical controls to meet security and compliance posture goals.

Cyber Security Analyst **PerimeterX, Inc. (San Mateo, USA)** **11/2019 – 08/2021**

Worldwide leader in behavioural bot management protection for e-Commerce apps. | *https://perimeterx.com*

- Lead and mentor to customers and multiple internal departments, alike. Evolved an onboarding program for the WFH era.
- Specialties in technical integrations, data logging solutions, high-value item AIO software research, JavaScript supply-chain risk, and information processing and asset (cookie, scripts, etc.) identification questionnaires.
- Automated alerting patterns and data query through parameterisation and scripting in YAML, SQL, JS, and Python.
- Identified multiple specific key patterns in anomalous network & client-side data points from Petabyte-scale data, then synthesised these into backend detection models to prevent and terminate account takeover, fraud, and card theft.

Cyber Security Analyst (Intern) **Pipeline Security, K.K. (Tokyo, Japan)** **02/2019 – 07/2019**

Leading provider of DNS security intelligence feeds to the Asia-Pacific (APAC) region. | *https://pipelinesecurity.net*

- Researched internal risk vulnerability by configuring secure policies & installing updates for cloud-hosted virtual machines, and programming a BIND DNS server with Response-Policy Zones to examine SIEM data visualization by ELK.
- Transformed customer image by contributing four articles of how-to documentation and negotiating a redesign of knowledgebase and homepage with co-workers, while providing production support to three customer companies.
- Investigated a false-positive spam listing, due to an issue identified in a shared hosting provider's nameservers (NS).

Skills

Certifications / Licenses	AWS Cloud Practitioner (-2024); Microsoft Azure SysAdmin [Associate] (-2022); CompTIA Security+ / A+ (-2024), Mobility+ / CDIA+ (lifetime)
Operating Systems	Windows, Mac OSX, Linux (Fedora, ChromeOS, Debian, CentOS, Android, Ubuntu)
Programming, Scripting	UNIX bash, SQL, VCL, JavaScript, Python, HTML, TOML/YAML, JSON, Java, Ruby
Programs / Toolkits	AWS/CloudFormation, Fastly, Google APIs, BigQuery, VMWare, Prometheus, ELK, CircleCI, git, SSH, homebrew, Insomnia, DNS/BIND, DMARC, Android Studio, JIRA
Websites Created / Contributed	https://madicetea.me [2018-] https://peakstudentcouncil.org [-2019], http://tokyo.hackjunction.com [-2017]
Accomplishments	GitHub Hacktoberfest Winner (2018 - 2021), CircleCI Orbtoberfest Winner (2020), ICMCP Black Hat Scholar (2017)

Education

The University of Tokyo [UTokyo] **(Tokyo, Japan)** **09/2015 – 09/2019**

Bachelor's Degree in Environmental Science **Minors** in Informatics & Science and Technology Studies